WinLock

User's Manual

Copyright © Crystal Office Systems. All rights reserved.

www.crystaloffice.com

Windows is a registered trademark owned by Microsoft Corporation.

All other mentioned trademarks can be registered trademarks of their respective owners.

THIS DOCUMENTATION IS PROVIDED «AS IS». THERE ARE NO EXPLICIT OR IMPLIED OBLIGATIONS, CONFIRMATIONS OR WARRANTIES, INCLUDING THOSE RELATED TO SOFTWARE MARKETABILITY AND SUITABILITY FOR ANY SPECIFIC PURPOSES, TO THE DEGREE OF SUCH LIMITED LIABILITY APPLICABLE BY LAW.

License for use and distribution

WinLock is distributed as try-before-you-buy. This means:

1. All rights to WinLock are exclusively owned by the author - Crystal Office Systems.

2. Anyone may use this software during a test period of 30 days. Following this test period of 30 days or less, if you wish to continue to use WinLock, you should purchase a license.

3. Once registered, the user is granted a non-exclusive license to use WinLock on as many computers as defined by the licensing terms according to the number of licenses purchased, for any legal purpose. The registered WinLock software may not be rented or leased, but may be permanently transferred, if the person receiving it agrees to terms of this license. If the software is an update, the transfer must include the update and all previous versions.

4. The WinLock evaluation version, may be freely distributed, with exceptions noted below, provided the distribution package is not modified.

5. To register you must complete the online registration form and pay registration fee.

6. WINLOCK IS DISTRIBUTED "AS IS". NO WARRANTY OF ANY KIND IS EXPRESSED OR IMPLIED. YOU USE AT YOUR OWN RISK. THE AUTHOR WILL NOT BE LIABLE FOR DATA LOSS, DAMAGES, LOSS OF PROFITS OR ANY OTHER KIND OF LOSS WHILE USING OR MISUSING THIS SOFTWARE.

7. You may not use, copy, emulate, clone, rent, lease, sell, modify, decompile, disassemble, otherwise reverse engineer, or transfer the licensed program, or any subset of the licensed program, except as provided for in this agreement. Any such unauthorized use shall result in immediate and automatic termination of this license and may result in criminal and/or civil prosecution.

   All rights not expressly granted here are reserved by Crystal Office Systems.

8. Installing and using WinLock signifies acceptance of these terms and conditions of the license.

9. If you do not agree with the terms of this license you must remove WinLock files from your storage devices and cease to use the product.

Contents

Chapter 1. Introduction 5
About WinLock 5
Key features 7
Why choose WinLock? 8
System requirements 9
Feature comparison for Windows editions 10
Chapter 2. Basics 11
Installing WinLock 11
Configuring user accounts 12
Remote Administrator 16
Checking for updates 17
Uninstalling the software 18
Chapter 3. Getting started 19
Overview 19
Launch WinLock 21
Enable WinLock 22
Tray pop-up menu 23
Enter WinLock password 24
Pause protection 25
Shutdown 26
Guest password 27
Password recovery 28
LockBox 29
Chapter 4. Settings 30
Configure WinLock 30
Protection 32
Settings 33
Notifications 35
Logging 36
Remote Administration 38
Security 39
Explorer and Windows 42
Start menu and Taskbar 43

Desktop 45
Mouse and Keyboard 46
Drives 47
User Account Control 48
Internet Explorer 49
Trusted sites 51
Restricted sites 52
Windows 53
Trusted executables 54
Restricted executables 55
Files 56
Folders 57
Timer settings 58
Chapter 5. Tips and features 60
Disable file download 60
Block Web browser 61
Disable the End Process command 62
Desktop icons protection 63
Kiosk mode 64
Command line parameters 65
Appendix A. Purchase and technical support 66
Purchase 66
Technical support 67

Chapter 1. Introduction

About WinLock

WinLock is a comprehensive security solution for personal or publicly accessible computers running all versions of Windows from 2000 to Windows 8. It is a program that ensures that only authorized people can access sensitive information on your computer.

With WinLock you can control how long others can use your computer. It runs from the system tray and requires a password to gain access to the available settings. It loads automatically with Windows and allows you to add an optional startup message, provide audio notification, and set the time limit. Once that limit is reached, Windows is summarily shut down. You can toggle the timer on and off from the tray. When enabled, there is no way around it without the proper password.

WinLock also allows to disable Windows hot keys (such as Alt-Ctrl-Del, Alt-Tab, Ctrl-Esc, etc.), lock Windows desktop, customize Start menu, hide Start button and Switch bar, and much more...

Block Windows and Lock Files features allow to block virtually any application or any part of it (window, popup message, dialog box), Explorer Windows (My Computer, Recycle Bin etc.), and lock selected files. Restricted sites feature filters Internet content and prohibits access to questionable websites.

Whether you're worried about coworkers going on the network and gaining unauthorized access to your private files, or your kids messing up your work files, WinLock is a software-only solution to your security needs.

WinLock is available in two editions: **Standard** and **Professional**. WinLock Professional offers all features of the WinLock, plus several advanced security capabilities of interest to the professional users. The advanced features of the Professional edition are:

- Ability to apply different restrictions separately to each user account.
- Internet Explorer restrictions.
- Search through website for prohibited keywords.
- Onscreen countdown timer.
- Built-in file encryption.

Key features

- **System restrictions** - disable command prompt, Desktop, Control Panel, Safe Mode, and more...
- **Parental control** - control how long your children can use the computer.
- **Restrict Start Menu** - hide the selective Start menu items, block context menus.
- **Control Internet access** - allow access only to the trusted sites only, and block all others.
- **Software filter** - block access to the downloaders, games, messaging clients, or CD burners.
- **Kiosk mode** - lockdown security for ATMs, terminals and public-access computers (companies, schools, hotels, public agencies).
- **Installation blocker** - prevent users from installing the software.
- **Hide drives** - hide your system and network drives in Windows Explorer.
- **Window blocking** - block virtually any application or any part of it: window, popup message, dialog box.
- **Logging** - monitor changes to the Windows shell and writes these changes to the log file.

and more to explore and use...

Why choose WinLock?

- **WinLock is suitable for a wide range of computer security tasks.**
  You can stop other users of your computer from peeking into your personal files. You can allow specific users to run a program while denying it to others. You can allow users to store their documents on removable drives, while preventing them from using unauthorized programs on those drives.

- **WinLock is easy to use.**
  WinLock sports one of the most intuitive user interfaces, that makes it easy to use by both novice users and computer professionals.

- **WinLock runs on a wide range of Windows platforms.**
  From Windows 2000 to Windows 8, with all service packs and hotfixes, all are supported by WinLock.

- **WinLock is widely used.**
  Hundreds of thousands of copies of WinLock have been downloaded by computer users from virtually all countries of the world.

- **WinLock will save you hours of learning time.**
  You don't have to learn how to use the Group Policies, user groups, Access Control Lists, privileges, and other built-in security features of Windows, because WinLock does the hard work for you: its visual and intuitive user interface lets you manage the restrictions with ease.

- **WinLock is widely used.**
  Hundreds of thousands of copies of WinLock have been downloaded by computer users from virtually all countries of the world.

- **WinLock is not a toy.**
  WinLock is used by large corporations and small businesses, schools and police departments, universities and correctional facilities, libraries and hospitals (to name a few).

- **WinLock is extensible.**
  You can fine-tune the access rules by creating appropriate security profiles.

- **WinLock is actively maintained.**
  Since its first release, we've been continuously extending, enhancing, and improving WinLock.

System requirements

- Any PC computer running Windows 2000 and higher.
- At least 9 MB of free space on the hard disk.
- A TCP/IP capable network (for remote administration).

Feature comparison for Windows editions

Some features and commands are available only on computers running the Windows Vista and higher. The following table summarizes the main differences in operation of WinLock under different editions of Windows.

Feature	Windows 2000 and XP	Windows Vista and 7	Windows 8 and higher
Disable preview pane	✗	✓	✓
Disable New Shortcut wizard	✗	✓	✓
Disable Address and Search bar	✗	✓	✓
UAC settings	✗	✓	✓
Disable Start screen	✗	✗	✓
Disable edge panels	✗	✗	✓
Disable Windows 8 tiles	✗	✗	✓

Chapter 2. Basics

Installing WinLock

If you already have a previous version of WinLock running on your computer, you should shutdown it before installing the upgrade.

To install WinLock:

- Log on as administrator.
- Follow the prompts to complete installation.
- Use **/silent** command line parameter to install in silent mode.
- Althrough you can change destination folder during setup, it is highly recommended to install WinLock into default location under **Program Files** folder.

Note: at this point WinLock, although installed, in no way affects the operation of your computer. To enable the protection you must run WinLock and use its commands to specify how exactly you want your computer to be protected.

Configuring user accounts

If you are working in a multi-user environment and want to use WinLock under new restricted user account, you need to configure system access permissions. To do this, you should move this user account to administrators group, then log on under this account and run WinLock. Finally, you can remove this account from administrators group.

Alternatively, under **General / Protection** click **Fix** button to adjust the access permissions automatically (works in Windows XP and higher). User Account Control should be turned on. If you are using Windows XP, administrator's password should not be blank.

If you don't see the Fix button, there is no need to configure the account.

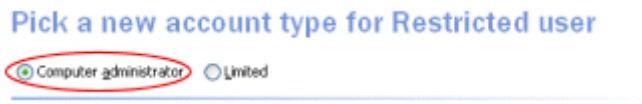
Or, download Account Configuration utility from our website. Select account under **Account** and click **Proceed**. Command line usage: *aconfig.exe <username>* or *aconfig.exe all_users*.

Later, you can apply the active settings to any user using **Profile / Apply**.

Windows XP

- Make sure you are logged on as **administrator**.
- Shutdown WinLock.
- Open Control Panel and click **Users Accounts**.
- Click **Change an account** and select **"Restricted User"**.

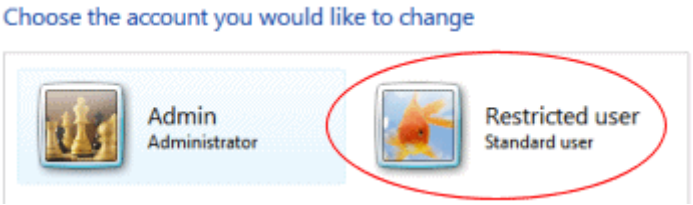
- Click **Change the account type** and select **Computer administrator**.



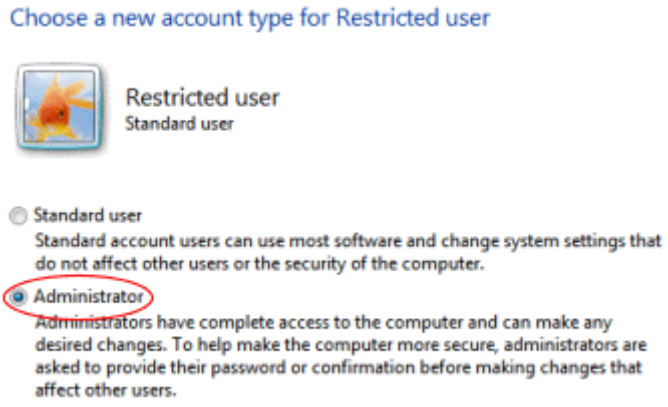
- Log on under **Restricted User** and run WinLock.
- Log on under **Administrator** account, and select limited account type for **"Restricted User"** account.

Windows Vista, Windows 7, and Windows 8

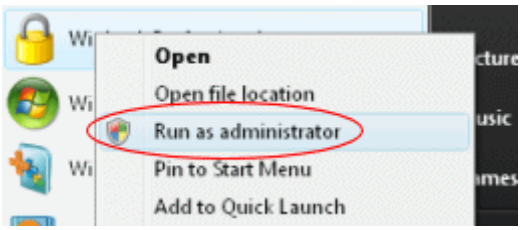
- Make sure you are logged on as **administrator**.
- Shutdown WinLock.
- Open Control Panel and click **Users Accounts**.
- Click **Manage another account** and select **"Restricted User"**.



- Click **Change the account type** and select **Computer administrator**.


Choose a new account type for Restricted user
Restricted user
Standard user
Standard user
Standard account users can use most software and change system settings that do not affect other users or the security of the computer.
Administrator
Administrators have complete access to the computer and can make any desired changes. To help make the computer more secure, administrators are asked to provide their password or confirmation before making changes that affect other users.

- Log on under Restricted User.
- Right-click WinLock icon in Start menu and click **Run as administrator**.

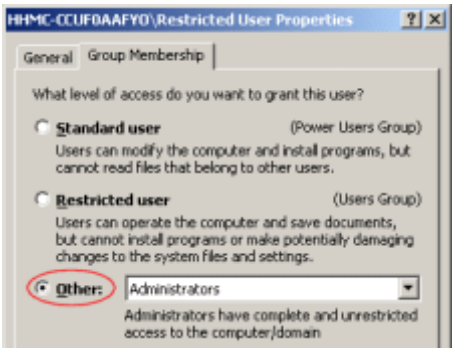


- Log on under **Administrator** account, and select standard user account type for **"Restricted User"** account.

Windows 2000

- Make sure you are logged on as **administrator**.
- Shutdown WinLock.
- Open Control Panel and click **Users and Passwords**.
- In Users and Passwords dialog select **"Restricted User"** account and click **Properties**.

- In User Properties dialog select **Group Membership** tab and add this user to administrators group.


HHMC-CCUFDAAFYO\Restricted User Properties
General
Group Membership
What level of access do you want to grant this user?
Standard user
(Power Users Group)
Users can modify the computer and install programs, but cannot read files that belong to other users.
Restricted user
(Users Group)
Users can operate the computer and save documents, but cannot install programs or make potentially damaging changes to the system files and settings.
Other:
Administrators
Administrators have complete and unrestricted access to the computer/domain

- Log on under **Restricted User** and run WinLock.

- Log on as **Administrator**, and select limited account type for **"Restricted User"** account.

Remote Administrator

WinLock Remote Administrator, the centralized remote management solution. It helps quickly configure remote WinLock clients via network, lock remote workstations, and apply security profiles by means of easy-to-use interface.

Being a client-server application, Remote Administrator allows the administrator to control the network installations of WinLock without leaving the computer. By means of this tool, administrators can manage WinLock settings, enable or disable each copy of WinLock separately, send pop-up messages and much more. With comprehensive encrypted protocol Remote Administrator allows fast and secure communication between multiple machines and can be safely deployed in any environment.

For more information about WinLock Remote Administrator please visit our website at http://www.crystaloffice.com.

Checking for updates

We are committed to providing updates and improvements to our software, and delivering them to our customers. You can use the Check for Updates feature to ensure that your copy is the most up-to-date version available. You must be connected to the Internet to use this feature.

To check for updated software:

- In main menu, click **Help**.
- Click **Check for Updates**.

Uninstalling the software

To completely uninstall WinLock, you CANNOT simply delete all the program files. If you wish to uninstall WinLock, follow these instructions:

- Right-click on the WinLock tray icon and click **Shutdown**. Then enter the correct password and click **OK**.

  It is necessary to shutdown WinLock before uninstall it!

- Click the Start menu from the taskbar and select Control Panel.
- Double click on Add/Remove Programs or Programs and Features.
- Select WinLock Professional from the list and click the Add/Remove button or Uninstall button.
- Confirm that you want to uninstall WinLock.

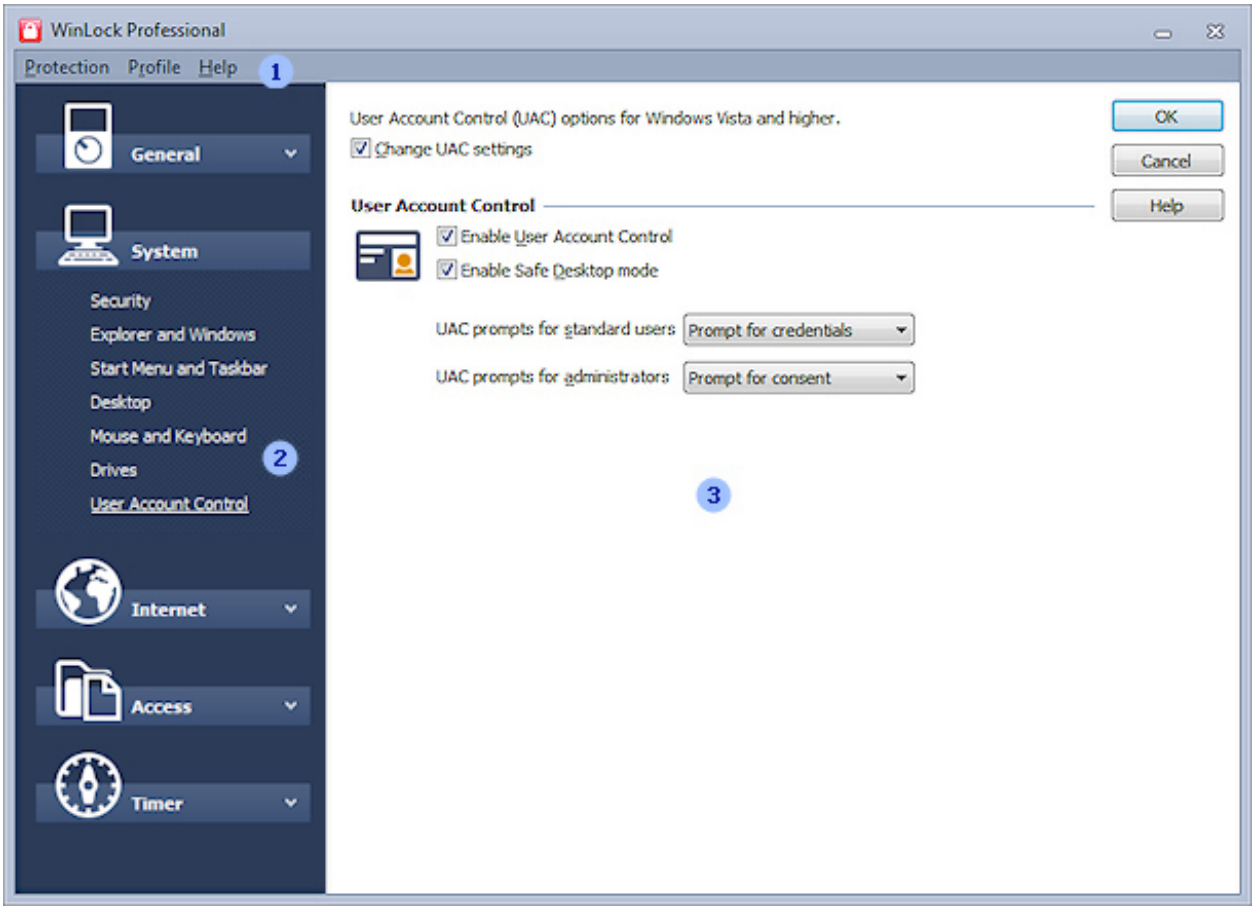
Chapter 3. Getting started

Overview

All WinLock commands are related to the following features:

- Restricting the access to system options.
- Locking system resources (applications, files, folders, etc.).
- Internet restrictions.
- Controlling how long others can use your computer.
- Monitoring the changes to the Windows shell.
- Remote administration.

The main window of WinLock looks like the following:



Numbers in this picture show the main parts of the program:

1. Main menu.
2. Shortcut bar.
3. Application area.

The Shortcut bar displays folders: General, System, Internet, Access, and Timer. Clicking on a folder makes that folder active and displays the icons it contains. Selecting an icon changes the page displayed in the application area.

Launch WinLock

First of all, a word of warning: WinLock is a powerful tool and should be used **responsibly**. Using it thoughtlessly, you can inadvertently make your computer inaccessible. For example, it is very easy with WinLock to prevent access to the desktop, and make Windows start with a blank screen after you reboot.

To launch WinLock click Start button then select Programs and click WinLock. After you start WinLock its icon appears in the system tray near the clock. It is good idea to use **Run as Administrator** command to run WinLock for the first time.

Note: by default, WinLock loads automatically on Windows startup.

Enable WinLock

After installation WinLock starts in Disabled mode. It means that all WinLock protection options are disabled. If WinLock is disabled, the tray icon is grayed.

- Right-click on the WinLock tray icon and select Enable item.
- You will be prompted for the password. Enter the correct password and click OK. Now WinLock is enabled.
- To disable WinLock right-click on the WinLock tray icon and select Disable item.

Tray pop-up menu

T Tray pop-up menu allows you to access the main WinLock functions. Right-click on the WinLock tray icon to open pop-up menu.

Pop-up menu contains the following commands:

- **Open WinLock** - opens WinLock main window.
- **Enable / Disable** - enables or disables WinLock protection.
- **Help** - displays the help contents page for WinLock.
- **Pause** - pauses protection.
- **Shutdown** - disables all forms of WinLock protection and unloads it from memory.
- **Shutdown Windows** - shutdowns Windows dialog.

Enter WinLock password

First, you should enter new WinLock password. Right-click on the WinLock tray icon and click **Open WinLock**. If you are using WinLock for the first time, you will not be asking for the password.

In **General** click **Settings**, enter password in **Password** and re-enter this password in **Confirm password**. Then click **OK**.

Letters in password must be typed using the correct case. Make sure that Caps Lock is not accidentally on.

REMEMBER THIS PASSWORD! You will be unable to configure or shutdown WinLock without it!

Pause protection

- **Pause for the specified time:** mode of resuming the protection which automatically enables protection in the specified time interval.

- **Pause until reboot:** mode which enables the protection after reboot of the operating system.

- **Disable protection:** enables protection only if you decide to resume it.

Shutdown

To shutdown WinLock, right click on the WinLock tray icon and click **Shutdown**. Or, open main window and click **Shutdown** in **Protection** menu (in this case you will be able to select the shutdown options).

- **Shutdown WinLock** - disables all forms of WinLock protection and unloads it from memory.
- **Shutdown Windows** - ends your session and shutdown Windows so that you can safely turn off power.
- **Restart Windows** - ends your session, shutdown Windows, and starts Windows again.
- **Logoff current user** - ends your session, leaving the computer running on full power.

Guest password

Guest password allows users to unlock the system locked by WinLock without entering the master password. Guest password can't be used to shutdown WinLock or change protection settings . Select **One-time password** to reset the guest password after the first use.

Password recovery

The Password recovery can help you restore control of WinLock if you ever forget its password. To recover your password, right-click WinLock tray icon and enter your license key in the password prompt. Be sure to enter the key EXACTLY as it appears in the message that you have received from us after you have purchased your license. This step is necessary to prevent unauthorized users from using the Password recovery to disable the protection performed by WinLock.

If you disabled WinLock tray icon and can't remember your hot key, try to do the following:

- Try to use the default **F11** hot key to open WinLock,
- or click **Start / Run** and run WinLock with **-open** command line parameter,
- or use this utility to restore the tray icon: http://www.crystaloffice.com/showicon.exe

LockBox

You are likely to have confidential documents on your computer, which you may want to encrypt. WinLock uses a very strong Blowfish crypto-algorithm, to protect data.

To open LockBox, In **Tools** menu click **LockBox**.

To encrypt a file, you will have to do the following:

- Select **Encrypt a file**.
- Enter the name of the file that you want to encrypt.

Tip: you can select multiple files by clicking on a file names while holding Ctrl key in Open dialog.

- Enter the password in **Password**, and re-enter it in **Confirm password**.

Tip: to use current WinLock password for encryption, select **Use WinLock password**.

- Select, whether you want to delete the source file after encryption.
- Click the **Next** button to encrypt the file.
- Your file is now encrypted and can be decrypted only by those who possess the password for that particular file.

To decrypt previously encrypted file, you will have to do the following:

- Select **Decrypt a file**.
- Enter the name of the file that you want to decrypt.
- Enter the password in **Password**.
- Select, whether you want to delete the source file after decryption.
- Click the **Next** button to decrypt the file.

Chapter 4. Settings

Configure WinLock

Normally, WinLock is displayed as an icon near the system clock.

Right-click on the WinLock tray icon and click **Open WinLock**. You will be prompted for the password. To adjust various WinLock settings, select an icon in the Shortcut bar. The corresponding page will be displayed in the Application area that takes up the main portion of the window area.

Note: if you are using WinLock first time, you will not be asking for the password.

The Shortcut bar displays folders: **General**, **System**, **Internet**, **Access**, and **Timer**.

Profiles

You may save WinLock settings to a file and open them later using the appropriate command in **Profile** menu. Using the profiles lets you to switch between different protection schemes easily. If you want to save current password in the saved profile, select **Save Password** in **Settings**. Also, profiles can be loaded on-the-fly from the command line without opening configuration window. For example, run **winlock.exe -profile internet.wlp <password>** (note that WinLock should be already loaded) to automatically apply internet.wlp profile.

To apply the profile to the other user, click **Profile** button and select **Apply**.

WinLock comes with a number of profiles ready for you to use. These predefined profiles located in **Profiles** folder and optimized for a particular purpose, defined by the profile name:

- **dialogs.wlp:** blocks system dialogs.
- **games.wlp:** blocks default games.
- **install.wlp:** disables software installation.
- **internet.wlp:** stops internet-related applications.
- **kiosk.wlp:** turns on kiosk mode. This mode allows the use of the one specific application, while disabling access to other programs and system resources. The shortcut to this application should be added into **Start\Programs\Startup** folder.
- **media.wlp:** disables multimedia applications usage.
- **msg.wlp:** avoid users from running common instant messengers.
- **p2p.wlp:** avoid users from running common file sharing peer2peer applications.
- **system.wlp:** restricts access to system settings.

Protection

This page allows you to configure protection options.

- **Enable protection** - clear this check box to temporarily suspend all forms of WinLock protection.

- **Password** - here you can enter or change WinLock password. It is not recommended to use as a password anything that is easy to guess (for instance, surnames, names, dates of birth). To ensure a secure password, use upper and lower case characters, figures and symbols.
  This password grants you access to WinLock settings. Be sure to select one that you will remember, but that no one will guess.

Users

Here you can create different protection schemes for each user account in a multiple-user environment. For each user, WinLock will activate only the selected restrictions. Moreover, it is possible to suspend all forms of WinLock protection for the specified user.

Let's say you have user account called **"Restricted User"** and you want to apply specified security restrictions to this account.

- Select **Use separate security settings for each user account** check box.

- Log on under the **"Restricted User"** account. You will see **Restricted User** under **Current user**.

- Select security restrictions that you want apply to this user and click **OK**.

Tip: to delete all previously created profiles, click Reset Profiles button.

Settings

This page allows you to adjust general WinLock parameters.

- **Turn on protection on startup** - if you select this check box, WinLock will be automatically enabled on startup, even if it was previously disabled.

- **Prompt for the password on startup** - if checked, this option causes WinLock to prompt for the password on startup in order to use the computer.

  Note: this option disables startup notification.

- **Enable Shutdown Windows menu** - select to enable **Shutdown Windows** item in WinLock tray popup menu. By clicking this item it will be possible to shutdown or restart Windows without opening WinLock main window. This is useful if you have disabled the Start button and need to shutdown your system without entering WinLock password.

- **Save password in settings profile** - select this check box if you want to save password in the settings profile.

- **Show password prompt on top of the other windows** - select to prevent password prompt and unlock prompt dialogs from loosing keyboard focus.

- **System monitoring** - if you select this check box, WinLock will continually monitor user activity to prevent changes that may affects WinLock security options.

- **Hide tray icon** - select this check box to disable WinLock tray icon. Note that pressing the **Properties** hot key will be required to show WinLock. Or, open folder where WinLock was installed and run **winlock.exe** file with **-showicon** parameter.

- **Unload protection** - prevents the ability to unload WinLock using third-party task managers.

- **Self-protection** - self-protection is used to enable the application's mechanism which protects its own files on the drive and its processes in memory. Note: you must restart your computer to make effect.

- **Ask for password to run restricted executables** - select to run the restricted executables after entering the correct password.

- **Automatically check for updates** - automatically checks for program updates.

- **Priority** - this setting lets you adjust WinLock's use of machine resources High priority improves the protection but may slightly slow down the computer. If you do not use System Monitoring, or Block Windows feature, you can select Low priority.

- **Language** - selects the program language.

- **Properties hot key** - select the hot key that opens WinLock main window.

- **Protection hot key** - select the hot key that enables or disables WinLock protection.

  Tip: to setup a hot key, click in the hot key box and press the desired keys, the box will update with the names of the keys you wish to use.

Notifications

Controls notification messages appearance.

- **Notification when application or site is blocked** - this warning message will be displayed each time application of website is blocked.
- **Notify on startup** - when timer is turned on, WinLock shows **"Time remaining"** messages on the system startup.
- **Show timer notification** - displays notification messages before shutting down the system.
- **Fade effect** - controls the fade-in animation of notification messages.
- **Show notifications as balloon hints** - select this check box to display notifications as pop-up balloon hints instead of notification messages.

Sounds

Various sound effects. Sound will be played even if the corresponding visual notification is disabled.

Logging

Logging feature monitors changes to the Windows shell, writes these changes to the log file, and optionally sends notifications to remote administrator. The following modes are available:

- **Disabled** - disables logging.
- **Log only** - writes event to log file.
- **Notify only** - sends notification to remote administrator.
- **Log and notify** - sends remote notification and saves event to log.

Click on the check box to enable or disable logging for the specified event. If the check box is checked, then the event will be logged.

Note: logging feature doesn't monitor console applications.

- **File created** - a new file was created, or website opened in Internet Explorer.
- **File changed** - an existing file was changed.
- **File renamed** - an existing file was renamed.
- **File deleted** - an existing file was deleted. Note: files that are sent to the Recycle Bin are excluded from logging on some operating systems.
- **Folder created** - a new folder was created.
- **Folder renamed** - an existing folder was renamed.
- **Folder deleted** - an existing folder was deleted.
- **Folder updated** - an existing folder content was updated.
- **Folder shared** - an existing folder was shared.
- **Folder unshared** - an existing folder was unshared.

- **Media inserted** - a new media was inserted into the drive.
- **Media removed** - a existing media was removed from the drive.

- **WinLock started** - WinLock was started (this event also logs the name of the current user).

- **Status changed** - WinLock was enabled, disabled, shutdowned, or the active session has been closed.

- **Computer locked** - the access to computer was locked by WinLock.

- **Website blocked** - the restricted website was blocked.

- **Executable blocked** - the disabled executable was blocked.

- **Application blocked** - the disabled window was closed.

- **User logged** - an user has been logged on using fast user switching, or the active session has been closed.

Click **Select Al**l or **Select None** to enable or disable logging of all events.
Click **View Log** to view events log.

Limit logging

Select **Limit logging** to set the limit on events to be logged. For example, if user deletes 500 files and limit is 10 events, only first 10 files will be logged. This is useful, when you don't need to know every file that was deleted, only that one or more files was in fact deleted. This is useful, when you don't need to know every file that was deleted, only that one or more files was in fact deleted

File size

Specified the maximum size in kilobytes to which log file can grow.

Remote Administration

This page provides access to WinLock Remote Administrator connection properties.

WinLock Remote Administrator, the network security solution for TCP/IP networks. A new security application that will make networks safer and administrators' life easier. Remote Administrator provides remote configuration of WinLock and WinLock Professional clients by means of a comfortable and easy-to-use interface.

WinLock Remote Administrator enables the administrator to control the network installations of WinLock without leaving the computer. By means of a fast and secure communication technology, administrators can manage WinLock settings, enable or disable each copy of WinLock separately, send pop-up messages, take remote desktop screenshots, and much more..

- **Enable remote administration** - select to enable remote control of this copy of WinLock.

- **Port** - identifies the port number used by WinLock Remote Administrator for connection to this computer. The port number must be identical to the value that was entered in the Remote Administrator's host list.

- **Use alternative password** - to gain the access to the remote host, Remote Administrator sends the access password with each command. Clear this check box if you want to use master password for remote control, otherwise enable this option and enter an alternative password in Password.

- **Accept commands from specified address only** - select this check box if you want to enable remote control from specified computer only, otherwise WinLock can be controlled from any network computer.

- **Remote address** - name or IP address of remote administration server.

Note: WinLock uses port 4000 for remote notifications, so this port should not be blocked by firewall software.

Security

This page provides access to the system security options.

General

Here you can adjust general security options.

- **Disable Registry Editor** - disables the Windows Registry Editors, **regedt32.exe** and **regedit.exe**.
- **Disable Display Properties** - prevents Display in Control Panel from running.
- **Disable Windows Update** - select this check box to prevent users from connecting to the Windows Update website and remove the Windows Update hyperlink from the Start Menu and from the Tools menu in Internet Explorer.
- **Disable programs on Settings menu** - prevents Control Panel, Printers, and Network and Dial-up Connections from running, and removes the corresponding menu items from Start menu.
- **Disable New Shortcut wizard** - disables the ability to create new shortcuts in Windows Vista and higher.
- **Disable shortcuts** - locks shortcuts.
- **Don't save settings on exit** - prevents users from saving certain changes to the desktop. Users can change the desktop, but some changes, such as the positions of open windows and the size and position of the taskbar, are not saved when users log off.

Advanced

An extra security options.

- **Disable Task Manager** - disables the ability to start Task Manager to view processes, applications running, and make changes to the priority or state of the individual processes.

- **Disable Control Panel** - prevents Control Panel from running.

- **Disable Lock Computer** - prevents users from locking the system.

- **Disable safe mode** - disables the ability to boot in safe mode. Safe mode is a special diagnostic mode of Windows, which you can use to troubleshoot problems with your computer. When you reboot your computer in the safe mode, only the core Windows components are loaded and activated. We **DO NOT** recommend enabling this option, because you may not be able to use the safe mode to troubleshoot the problems. Use this option at your own risk. Note: this option disables safe mode in Windows 2000 and higher. To disable safe mode in Windows 98, use Boot feature.

- **Disable My Computer** - removes My Computer icon from desktop and Start menu.
- **Disable command prompt** - disables the ability to run the interactive command prompt, **cmd.exe**.

- **Disable system properties** - disables System properties dialog.

- **Disable Programs and Features** - removes Programs and Features and Add/Remove Programs from Control Panel and menus.

- **Disable Change Password** - disables the Change Password button on the Windows Security dialog box (which appears when you press Alt-Ctrl-Del).

- **Hide Fast User Switching** - removes Switch User option from the Alt+Ctrl+Del screen.

- **Disable Computer Management** - disables Computer Management console.

- **Disable Run as Administrator** - removes Run as Administrator item from Explorer context menu.

- **Enable Shutdown Event Tracker** - enables Shutdown Event Tracker. Shutdown Event Tracker is a Microsoft Windows Server feature that you can use to consistently track the reason for system shutdowns.

- **Disable Windows Installer** - disables Windows Installer. No installs are allowed including repairs, reinstalls, or on-demand installations.

Explorer and Windows

This page includes a group of options that restrict Explorer and windows-management commands.

- **Hide menu** - select this check box to remove Windows Explorer main menu or ribbon.
- **Hide Folder Options menu** - removes the Folder Options item from all Windows Explorer menus.
- **Disable context menu** - select this check box to disable Explorer right-click context menu.
- **Hide search button** - removes search button from Windows Explorer under Windows 2000 and XP, or removes search and task view from Windows 10 task bar.
- **Disable Map/Disconnect** - select this check box to remove the Map Network Drive and Disconnect Network Drive options.
- **Disable Address and Search bar** - disables Explorer Address bar and Instant Search box (available in Windows Vista and higher).
- **Disable preview pane** - disables the preview pane in Open dialogs. Available in Windows Vista and higher.
- **Disable Close command** - disables the ability to close windows.
- **Disable Move command** - disables the ability to move windows.
- **Disable Resize command** - disables the ability to resize windows.
- **Disable Restore command** - disables the ability to restore windows.
- **Disable Maximize command** - disables the ability to maximize windows.
- **Disable Minimize command** - disables the ability to minimize windows.
- **Disable main menu** - prevents user from being able to open main and window menus (may not work with some programs).

Start menu and Taskbar

Click on the check box to show or hide Start menu items. If the check box is checked, the corresponding menu item will be shown in Start menu. If the check box is unchecked, the corresponding menu item will be removed from Start menu.

- **Hide recent programs** - removes frequent programs list from the Start menu.
- **Hide all programs** - removes the More Programs list from the Start menu.
- **Hide user name** - remove user name from Start menu (Windows XP only).
- **Disable drag and drop** - disables drag and drop on the Start menu.
- **Disable Start menu** - hides Start menu but retains the access to Start button right-click menu (Windows 10 only).
- **Disable Start screen** - disables Windows 8 Start screen.
- **Disable Start button** - hides the Start button.
- **Hide Switch bar** - select this check box to hide the portion of the taskbar where you find all the buttons of active applications.
- **Lock taskbar** - restricts users from making any changes to taskbar position.
- **Hide taskbar** - select to hide the entire taskbar, including Switch bar, system tray, and Clock. The **Auto-hide the task bar** option in taskbar properties should be turned off.
- **Hide tray items** - select to hide the system tray icons.
- **Hide tray context menu** - removes the context menus for the tray, including the Start button, Selection bar, and clock.
- **Disable taskbar customization** - this option will lock the option of pressing the Property from the mouse right click on the taskbar.
- **Lock taskbar's toolbars** - prevents users from adding, dragging, dropping and closing the taskbar's toolbars.
- **Disable taskbar redock** - prevents users from moving the taskbar.
- **Disable taskbar resize** - disables the ability to resize the taskbar.
- **Disable Start screen** - disables Windows 8 Start screen.
- **Disable Action Center** - disables Windows 10 Action Center.

- **Disable edge panels** - disables hot corners and popup edge panels in Windows 8.

Desktop

- **Block desktop** - select this check box to hide all desktop icons and shortcuts.
- **Disable Active Desktop** - select this check box to disable Active Desktop and prevent users from enabling it.
- **Read-only desktop icons** - select this check box to disable the ability to rename desktop icons in place. To completely disable desktop icons modification, use this option in combination with **Disable Explorer context menu**.
- **Disable HTML wallpaper** - permits only bitmap images for wallpaper.
- **Disable changing wallpaper** - disables all options on the Background tab of Display in Control Panel. As a result, users cannot add or change the background design of the desktop.
- **Hide Recycle Bin** - removes the Recycle Bin icon from the desktop. You must restart your computer to make effect.
- **Hide Network** - removes the Network icon from the desktop.

Mouse and Keyboard

Hot keys

Click on the check box to enable or disable the specified system-wide hot key (such as **Alt-Esc**, **Alt-Tab**, **Ctrl-Esc**, etc.). If the box is checked, then the corresponding hot key will be blocked.

Click **Disable All** to block all hot keys or Enable All to enable.

Tip: you cannot disable Alt+Ctrl+Del directly. However, you can disable all items under Alt+Ctrl+Del screen (Lock Computer, Change Password, Fast User Switching, Log off and Task manager). This will make this hot key useless.

Tip: to disable Flip 3D (Windows+Tab key) feature in Windows Vista and 7, use **Disable Windows key** option.

Mouse

Click on the check box to enable or disable the specified mouse button.

Click **Disable All** to block all buttons or **Enable All** to enable them.

Note: you will be able to use mouse buttons in the system tray in order to access WinLock tray icon unless **Hide tray icon** option is turned on.

Drives

General

Click on the check box to enable or disable the display of the drive in My Computer and Explorer. If the check box is checked, then the drive will be shown in My Computer and Explorer if the drive exists on the computer. If the check box is unchecked, then the drive will be removed from My Computer and Explorer.

- Click **Hide All** or **Show All** to hide or show all system drives.

Removable storage

- **Block access to removable storage** - select to block removable storage devices (CD ROMs, USB Drives, etc.).

User Account Control

This page provides access to Windows Vista, Windows 7 and Windows 8 User Account Control settings.

- **Enable User Account Control** - enables User Account Control.
- **Enable Safe Desktop mode** - this setting determines whether the elevation request will prompt on the interactive users desktop or the Secure Desktop.

UAC Prompts

This setting determines the behavior of the elevation prompt for standard users and administrators.

- **None** - elevate privileges automatically without prompt.
- **Prompt for credentials** - an operation that requires elevation of privilege will prompt the user to enter an administrative user name and password.
- **Prompt for consent** - an operation that requires elevation of privilege will prompt the user to select either permit or deny.

Internet Explorer

This page includes a group of options that control Internet Explorer restrictions.

- **Disable New command** - disables New Window command on File menu.
- **Disable Open command** - disables Open command on File menu.
- **Disable Save command** - disables Save and Save As on the File menu.
- **Disable Save As dialog** - prevents user from being able to select download folder by not displaying the Save As dialog box when a file is downloaded.
- **Disable Close command** - prevents user from being able to close Internet Explorer.
- **Disable printing** - removes Print and Print Preview from the File menu.
- **Disable Find Files** - disables the Find Files command.
- **Disable file download** - disables the ability to download files.
- **Disable Full Screen mode** - disables the Full Screen option.
- **Disable Windows 8 tiles** - always open the desktop version of Internet Explorer (Windows 8 only).
- **Disable View Source command** - disables the ability to view the page source.
- **Hide Favorites** - hides Favorites menu, and disables adding to adding to favorites, or organizing favorites.
- **Disable internet options** - disables Internet Options on the Tools menu.
- **Disable context menu** - disables right-click context menu.
- **Disable toolbars options** - disables adding, removing, or moving toolbars. For example, if you want to disable the ability to show Address Bar in both Internet Explorer and Windows Explorer, you should open Internet Explorer, hide Address Bar (View/Toolbars/Address Bar) and then select Disable toolbars options check box.
- **Hide navigation buttons** - disables the Forward and Back navigation buttons.
- **Disable History bar** - hides the History bar.

- **Disable Folders bar** - hides the Folders bar.

- **Disable Address and Search bar** - disables Address bar and Instant Search box in Internet Explorer 7 and above.

  Note: some of these options may affect Windows Explorer.

- **Restricted Sites** - specifies, whether restricted websites will be closed or redirected.

Trusted sites

This page provides access to the list of trusted websites.

Use this page to list the only websites that may be accessed. For example, add .edu into the trusted sites to allow access to all .edu websites. All other sites (regardless of the keywords they contain) will be unavailable.

Note: the Inline AutoComplete option in browser settings should be turned off.

Restricted sites

This page allows you to enter keywords or site address that can terminate web session. The **Professional edition** of WinLock not only checks the address of the site, but also scans the entire page, including the hidden meta-tags for any prohibited words. For example, if you define **"sex"** as a keyword, any website contains this word will be prohibited. This makes possible to prohibit access to questionable websites - notably for public-access computers in schools and libraries.

Tip: if you want to log each attempt to open prohibited website in log file, select **Add event to log** check box.

Windows

This page provides access to the Block Windows feature.

Block Windows can block any selected window or dialog, such as **My Computer**, **Control Panel**, **Internet Properties**, etc. For example, if you want to disable the ability to open **My Documents** window click Add button and enter **My Documents** in **Caption**.

Note: the caption is the title of the application while running it and not the application name! Look at the text in the application top line while running it and enter it in WinLock caption list.

Tip: use **Find Window** button to list all visible windows.

Tip: caption may contains ***** and **?** wildcards. A question mark matches any single character. An asterisk matches any number of occurrences of that string followed by any characters. For example, **bo*** matches **bot**, **bo** and **boo** but not **b**. So, if you want to block all windows with a caption that begins, for example with a **Internet** word, you can use the following string: **Internet***.

Trusted executables

This page provides access to the list of trusted executable files. Use this page to list the only executables that may be accessed. All other executables (except Windows core components) will be unavailable.

Tip: you can use ***** and **?** wildcards. A question mark matches any single character. An asterisk matches any number of occurrences of that string followed by any characters.

Restricted executables

Here you can block application by the executable name or version info. For example, the following application name would be used to close the Internet Explorer when someone tries to open it: **iexplore.exe**. File info contains version and copyright information about the file (company name, product name, comments, etc.) To read version information, right click the file in Windows Explorer and select **Properties/Version**. For example, each software product created by Adobe Systems contains word **Adobe** in version information. So, you can use the following string to disable the ability to open Adobe software at all: ***Adobe***. With executable blocking you can disable nearly all software installation packages. To do this, add ***setup*** and ***install*** into the File info.

Tip: both file name and version info may contain ***** and **?** wildcards. A question mark matches any single character. An asterisk matches any number of occurrences of that string followed by any characters.

Tip: select **Ask for password** option on the settings page to run the restricted executables after entering the correct password.

Files

This page provides access to the Lock Files feature. This feature is similar to restricted executables except it can lock any file, but not only applications.

Blocked files can't be opened for viewing or editing. Click **Add** button and enter file name in **File**. Or, you can drop the selected files from Explorer onto the locked files list. Also, you can use this feature to block any selected application. For example, if you want to disable the ability to open Internet Explorer, add the full path to its executable file **c:\Program Files\Internet Explorer\iexplore.exe** into the locked files list.

Check-mark at the left of the file name controls file protection mode:

- Select the check-mark to lock the file.
- Remove the check-mark from a file name to prevent the file from being locked.
- Select **Read-only access** to allow read-only access to the file.

Folders

This page provides access to the Lock Folders feature.

You can select folders you want to disable. These folders can't be opened, renamed or deleted.

Click **Add** button and enter folder name in **Folder**. Or, you can drop the selected folders from Explorer onto the locked folders list. Select **Allow read-only access to folder** to retain the read-only access to the folder.

Note: you can't lock folder if it is already opened by other application.

Tip: you can disable the access to the entire disk. For example, if want to disable the access to drive **D**, add **D:** string to the locked folders list. This will prevent the access to this drive, including all files and folders located on it.

Timer settings

Timer controls how long others can use your computer. Once that limit is reached, Windows is summarily shut down.

- **Enable** - select to enable timer.
- **Restart timer** - if elected, WinLock will reactivate the timer with a new value. This check box is disabled when timer is inactive.

  Tip: when enabled, WinLock displays the remaining time as a part of the tray icon hint.

- **Countdown timer** - select this option to start timer in countdown mode. Then, specify how long your computer will be available (for example, 3 hours and 45 minutes daily).
- **Time range** - specify the time range when your computer will be available (for example, from 9:00 am till 16:00 pm). All attempts to change the system time will be blocked.
- **Shutdown** - shuts down the system.
- **Logoff** - shuts down all running processes and logs the user off.
- **Lock** - locks the computer and opens Windows Welcome Screen. The timer will be disabled after unlock.
- **Lock after reset** - select this box if you want to lock Windows after incorrect shutdown (for example, after pressing the Reset button).
- **Disable timer after unlock** - select this check box if you want to turn the timer after unlock the computer.
- **Reset timer daily** - this option allows you to limit daily computer usage. When enabled, WinLock unlocks the computer for a certain period of time, once in a day. Do not attempt to adjust system date and time while this mode is active! Otherwise, the PC will be locked. It is also recommended to disable **Internet time synchronization** option.

  Note: this option is unavailable in **time range** mode.

- **Unlock prompt** - specifies how long WinLock shows the unlock dialog that prompts for the correct password on the startup.

- **Block attempts to reenter the password** - select to disable the ability to enter the password more than once. This prevents brute-force password cracking.

  Tip: to lock the computer immediately, in **Protection** menu select **Lock**.

Chapter 5. Tips and features

Disable file download

To disable the ability to download files from websites add **File Download** dialog into the blocked windows list.

- Open WinLock main window and select **Access / Windows** section.
- Add **File Download** caption into the blocked windows list.

Tip: in WinLock Professional use Disable file download option.

Block Web browser

The best way to block Web browser is to add its executable file into the blocked files list.

- Open WinLock main window and select **Access/Files** section.

- Add the full path to Web browser executable file into the locked files list. For example, **c:\Program Files\Internet Explorer\iexplore.exe** or **c:\Program Files\Opera\Opera.exe**.

Disable the End Process command

If you want to disable the ability to end processes from Windows Task Manager, but do not want to disable the Task Manager itself add **Task Manager Warning** into the blocked windows list.

- Open WinLock main window and select **Access/Windows** section.
- Add **Task Manager Warning** into the blocked windows.

Desktop icons protection

If you want to protect desktop icons but do not want to hide them, you can use Lock Files feature:

- Open **Access / Files** section.
- Click **Browse** button.
- Select Desktop folder and add all ***.lnk** files into the blocked files list.
- Select gray mark at the left of each file to allow read-only access.

Kiosk mode

Kiosk mode allows the use of the one specific application, while disabling access to other programs and system resources. To enable kiosk mode:

- Add shortcut to the application into **Start\Programs\Startup** folder.
- In main menu, click **Profile / Import**.
- Select **kiosk.wlp** profile.
- Enable WinLock.

Command line parameters

WinLock accepts the following optional command line parameters:

- **-open** - opens WinLock.
- **-enable <password>** - enables protection.
- **-disable <password>** - disables protection.
- **-password <password> <new password>** - changes WinLock password.
- **-cp <password>** - creates new WinLock password. Use this command to create password right after installation.
- **-lock <password>** - locks the computer.
- **-shutdown <password>** - shutdowns WinLock.
- **-showicon** - restores the tray icon.
- **-profile <profile file name> <password>** - applies settings profile. You can use this command right after installation when WinLock password is not created yet. In this case you don't need to enter the password in command line.

These command line options do not specify the startup options, but affects the active instance of WinLock. In other words, you should start WinLock first, and then use command line arguments to control its behavior.

Appendix A. Purchase and technical support

Purchase

You may try out WinLock without any costs for the period of 30 days. If you wish to keep on using it after this period, you should purchase a license.

Registration gains access to the some advanced features:

- Lock desktop.
- Hide taskbar.
- Self-protection.
- Ability to lock unlimited number of files and websites.
- One year of free upgrades.
- Free online technical and customer support.

If you wish to become a registered WinLock user, all you need to do is make a payment via online order page.

Online purchase available for all payment options, including Credit Card, PayPal, Fax, Check, Wire Transfer, and Purchase Order.

Technical support

Before you contact us, please do the following:

- Be sure that you're doing everything right. We all make mistakes sometimes: be attentive.
- Look at the Help file: it may already contain an answer to your question.
- Visit WinLock home page in the Internet at http://www.crystaloffice.com. It's a good chance that you'll find the newer version of WinLock there.

If you still have a problems with WinLock, or if you have questions or comments, please e-mail to support@crystaloffice.com. Make sure that your message contains a valid return address. In particular, be sure to remove the "anti-spamming" parts, if any, from your return address.

When reporting problems, please include the following information:

- Which OS are you running?
- WinLock version (see the "About" dialog).
- Description of the problem (as much detail as possible so we can duplicate the problem).

We'll try to help you as fast as possible, usually in one or two business days.

Feedback

We welcome your opinion about our software. Your feedback is important to us in order to get an idea of how to make our software a better product for you. So if you have a grand idea for a new feature, or a better way of doing something, please drop us a note. Please visit the WinLock home page to download the latest version and find out more about our software.